Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 9**

Temas: **Getting started with databases (lab), Cyber Security,Securing the cloud**

Integrantes:

Ramón Reyna García
Matrícula: 348411
a348411@uach.mx

Gabriel Isai Prieto Saenz
Matrícula: 353297
a353297@uach.mx

Gabriel Jesus Bustillos Fierro
Matrícula: 353267
a353267@uach.mx

1. Resumen Tema “Getting started with databases (lab)”

Las bases de datos son estructuras organizadas que almacenan y gestionan conjuntos de datos. La naturaleza de los datos puede variar desde texto simple hasta imágenes complejas o información financiera. Los fundamentos de las bases de datos incluyen la creación, acceso y manipulación de datos de manera eficiente. Hay varios tipos de bases de datos, como las relacionales, NoSQL y basadas en objetos, cada una diseñada para diferentes necesidades y estructuras de datos.

Amazon RDS (Relational Database Service) es un servicio en la nube que facilita la configuración, operación y escalabilidad de bases de datos relacionales en la infraestructura de Amazon Web Services (AWS). Configurar Amazon RDS implica seleccionar el motor de base de datos adecuado, como MySQL, PostgreSQL o SQL Server, y configurar parámetros como la capacidad de almacenamiento y la instancia de base de datos.

El uso de Amazon RDS proporciona numerosos beneficios, incluida la administración automatizada de tareas de mantenimiento, copias de seguridad y parches de seguridad. Además, ofrece opciones de escalabilidad para adaptarse a las demandas cambiantes de los datos y el tráfico. Los usuarios pueden acceder a sus bases de datos alojadas en Amazon RDS

mediante diversas herramientas y aplicaciones, lo que permite una integración fluida en sus entornos de desarrollo y producción. En resumen, Amazon RDS simplifica la gestión de bases de datos relacionales en la nube, brindando flexibilidad, escalabilidad y confiabilidad a los usuarios.

2. Resumen Tema “Cyber Security”

La ciberseguridad es un tema de creciente importancia en el mundo digital actual, donde la protección de datos y sistemas se ha vuelto fundamental para empresas, organizaciones y usuarios individuales. En este contexto, la nube ha surgido como un entorno clave donde se deben aplicar sólidas medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

Una de las áreas principales de la ciberseguridad es la gestión de identidades y accesos. Esto implica asegurar que solo las personas autorizadas tengan acceso a recursos y datos sensibles, mediante el uso de autenticación multifactor, gestión de contraseñas robustas y políticas de acceso basadas en roles. La implementación adecuada de estas medidas es crucial para prevenir brechas de seguridad y ataques de suplantación de identidad.

Otro aspecto clave es la protección de datos, que abarca desde la encriptación de información confidencial hasta la implementación de controles de acceso granulares. La encriptación garantiza que, incluso si los datos son interceptados, no puedan ser utilizados sin la clave de descifrado adecuada. Por otro lado, los controles de acceso aseguran que solo los usuarios autorizados puedan ver o manipular información sensible.

La monitorización de la seguridad es igualmente importante en el panorama de la ciberseguridad. Mediante la implementación de herramientas de monitoreo y detección de amenazas, las organizaciones pueden identificar actividades sospechosas o ataques en tiempo real, permitiéndoles tomar medidas correctivas de manera oportuna y mitigar el impacto de posibles brechas de seguridad.

Además de estas medidas técnicas, la concienciación y formación en seguridad cibernética son fundamentales. Educar a los empleados y usuarios sobre las mejores prácticas de seguridad, como la detección de correos electrónicos de phishing, el uso seguro de contraseñas y la actualización regular de software, contribuye significativamente a la protección global contra ciberataques.

En resumen, la ciberseguridad es un campo multidimensional que abarca la gestión de identidades y accesos, la protección de datos, la monitorización de la seguridad y la concienciación de los usuarios. La implementación efectiva de estrategias y tecnologías en

estas áreas es esencial para mitigar riesgos y proteger la información en el entorno digital actual.

3. Resumen Tema “Securing the cloud”

La seguridad en la nube es importante, y necesaria, ya que aunque una aplicación funcione sin seguridad, nunca falta algún listo que se quiera aprovechar de eso. En caso de haber recibido un ataque de hackers lo recomendado es cambiar las contraseñas lo más pronto posible, también se debería tener un backup o respaldo de información por si se llega a perder alguna data, la nube por si misma ya ofrece seguridad pero en el punto de su infraestructura, lo que sucede en la aplicación depende del desarrollador, como por ejemplo la administración de accesos y la autenticación del que quiere ingresar.

Tener un control de accesos nos asegura un buen control de quienes pueden hacer y no hacer, denegando acceso a quienes no deberían poder tener cierta información, aunado a esto relacionamos el Principio del mínimo privilegio, que habla acerca de dar privilegios o permisos mínimos indispensables para el rol del usuario, así tenemos un control de que hace cada quien sin otorgar permisos de innecesarios.

Además de implementar medidas básicas de seguridad como el cambio regular de contraseñas y la creación de backups, es esencial que los desarrolladores adopten prácticas de codificación segura y se mantengan al tanto de las últimas amenazas cibernéticas.